

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,)	CASE NO. 8:07CR199
)	
Plaintiff,)	
)	
v.)	BRIEF IN SUPPORT OF
)	OBJECTION TO MAGISTRATE
HAROLD STULTS,)	JUDGE'S REPORT AND
)	RECOMMENDATION
Defendant.)	

Harold Stults is charged with a violation of 18 U.S.C. §§ 2252(a)(4)(B) and 2252(b)(2). In essence, the Indictment charges Mr. Stults with possession of child pornography which had been placed in interstate commerce through a computer. The charges stem from a search warrant that was issued by the Honorable Thomas D. Thalken on February 27, 2007. The search warrant was based upon an Application and Affidavit for Search Warrant signed by Special Agent Brent Morral. Mr. Morral's affidavit relied heavily upon an investigation that was started by Special Agent Joseph Cecchini of the Federal Bureau of Investigation.

According to the Affidavit, on October 26, 2006, S.A. Cecchini "launched the P2P program, Limewire, and conducted a search using the term 'pthc.' Among the responses to the search term was one from IP address 24.252.31.129. At approximately 1208 (CDT), SA Cecchini used a user command for the individual using IP address 24.252.31.129. Subsequently, SA Cecchini was able to connect with said IP address and obtain a list of files that user was sharing." (Affidavit, ¶ 23(B)) The Affidavit of Agent Brent Morral continues in ¶ 23(C) and states that SA Cecchini "viewed the list of files available from IP address 24.252.31.129, which displayed several files with file names consistent with child

pornography. SA Cecchini subsequently initiated several downloads from the files listed beginning at approximately 1209 (CDT).”

In non-computer terminology, the above recitation of facts describes a warrantless search by an FBI agent into the computer files possessed by the Defendant at his home. There is no question that Agent Cecchini did not have a warrant at the time that he accessed Mr. Stults’ files on October 26, 2006. Further, it is undisputed that Mr. Stults had never communicated with Agent Cecchini to consent to search his computer files. Nevertheless, by Agent Cecchini’s actions, law enforcement was able to determine the contents of Mr. Stults’ computer, take files from his computer and view them all at a distant location. The Defendant contends that this action was done in violation of his rights under the Fourth Amendment to the Constitution of the United States.

There are few, if any, cases directly on point which the government can rely upon to justify law enforcement’s actions in this case. This case is roughly analogous to the facts in Murray v. United States, 487 U.S. 533 (1988). In Murray, police officers entered a warehouse without a warrant and observed bundles of marijuana. The officers later applied for a search warrant, but did not mention their illegal entry or observations made during the entry. The actual question in Murray was whether the search pursuant to the warrant was based upon an independent source not prompted by the illegal conduct. There was no disagreement that if the search warrant was indeed based upon the warrantless entry, the evidence would have been properly suppressed.

Here, there can be no independent source to justify the government’s actions. A review of the Application and Affidavit for Search Warrant reveals that the only possible basis for concluding that Mr. Stults’ computer may have contained evidence of child

pornography was obtained from SA Cecchini's downloading of files from Mr. Stults' computer.

The Report and Recommendation states that "the P2P network is a file sharing network that belies a reasonable expectation of privacy." The Application and Affidavit for the Search Warrant contains several pages of boilerplate language which attempts to explain in general the "growing phenomenon on the Internet" of "peer to peer file sharing." (§ 6(C)) The Affidavit also states that to access "P2P" a user downloads software from the internet. However, the Report and Recommendation fails to address the fact that the Affidavit does not indicate in any manner the agent's or affiant's knowledge of the computer programs on Mr. Stults' computer. For example, the Affidavit does not even state that Mr. Stults had "Limewire" installed on his computer, and if it was installed on his computer, when it was installed, by whom or the circumstances of that installation. These are important considerations because the Affidavit is completely without support for the assumption that Mr. Stults must have taken some voluntary action to permit others to view files on his computer and thereby gave up any expectation of privacy.

The Report and Recommendation shows a clear misunderstanding of certain aspects of the P2P "growing phenomenon." For example, the Magistrate Judge states that "a person has the ability to send files from his computer to another user's computer without permission or knowledge. . . ." Report and Recommendation, p. 2. In fact, the Affidavit at paragraph 6(I) indicates, in bold, just the opposite. At page five of the Report and Recommendation the Magistrate Judge states, "[A]bsent such an expectation [of privacy], the Fourth Amendment does not prohibit law enforcement officers accessing the P2P network and viewing files that have been downloaded by various IP address." Simply

stated, files are not downloaded by internet addresses. In this case, Mr. Stults is not alleged in the Affidavit to have downloaded any child pornography. SA Cecchini is stated to have downloaded images using the P2P software program. Also, the Report and Recommendation states that SA Cecchini was “looking for users accessing known child pornography sites.” *Id.*, p. 2. Instead, the agent “conducted a search using the term ‘pthc.’ He was not searching the internet for persons viewing child pornographic web sites.”

While other cases have discussed the obtaining of child pornography files over the Internet, none of the cases appear to answer the precise Fourth Amendment question in this case. For example, in United States v. Griffin, 482 F.3d 1008 (8th Cir. 2007), Griffin had downloaded child pornography from Kazaa, an Internet peer to peer file sharing network. However, none of the issues in Griffin implicated the Fourth Amendment. In United States v. Sewell, 457 F.3d 841 (8th Cir. 2006), the defendant also used Kazaa to download images of child pornography. Again, however, Sewell dealt with issues unrelated to how the government obtained the images from Sewell’s computer.

One important distinction from this case and Griffin and Sewell is the fact that the computer program “Kazaa” was used in both Griffin and Sewell, but not in this case. As thoroughly discussed by the Court in United States v. Shaffer, 472 F.3d 1219 (10th Cir. 2007), Kazaa is a computer program that permits Internet sharing. According to the decision in Shaffer, the installation process of Kazaa on an individual’s computer involves acceptance of a license agreement which acknowledges the capability of the program to place files on the internet available for downloading by other individuals.

Similarly, in United States v. Abraham, 2006 LEXIS 81006 (W.D. Pa. 2006), an Internet P2P program called “Bear Share” (rather than Kazaa) was used by the defendant

in connection with his possession of child pornography. The Court explained the defendant's actions in a thorough opinion. By contrast, the Affidavit in this case does not 1) mention the program used by Mr. Stults; 2) state Mr. Stults used a P2P program; 3) indicate Mr. Stults' acceptance of the terms of a software license agreeing to file sharing; 4) when such a program may have been installed on the computer; 5) whether use of such a program requires action on the part of Mr. Stults; 6) whether Mr. Stults was required to affirmatively indicate his files could be shared; or 7) even indicate whether Mr. Stults' computer had to be turned on to permit access to files. These are important considerations for the Court in determining whether Mr. Stults retained a reasonable expectation of privacy in his computer files.

Without stating specific facts pertinent to Mr. Stults' computer, there is no basis to conclude that SA Cecchini's actions complied with the Fourth Amendment. If in fact, SA Cecchini unlawfully searched Mr. Stults' computer first without a warrant, the good faith exception of United States v. Leon, 468 U.S. 897 (1984), should not apply (suppression appropriate where police engage in misconduct or were reckless in preparing affidavit. 468 U.S. at 926).

The Defendant asserts that the actions of SA Cecchini in this case amounted to a warrantless search without a valid consent and in violation of Mr. Stults' Fourth Amendment rights. For these reasons, Mr. Stults' Motion to Suppress must be sustained.

Respectfully submitted,

HAROLD STULTS, Defendant,

By: s/ David R. Stickman
DAVID R. STICKMAN
Federal Public Defender
222 South 15th Street, Suite 300N
Omaha, NE 68102
(402) 221-7896

CERTIFICATE OF SERVICE

I hereby certify that on November 13, 2007, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which sent notification of such filing to the following: Michael Norris, Assistant United States Attorney, Omaha, NE.

s/ David R. Stickman